

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Information associated with Google, LLC email account:
SHELTONSTAXSERVICE@GMAIL.COM that is stored at
premises controlled by Google, LLC, 1600 Amphitheatre
Parkway, Mountain View, CA 94043

Case No. 4:20 MJ 3172 NCC

SIGNED AND SUBMITTED TO THE COURT
FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. Section 287
26 U.S.C. Section 7206(2)

Filing False Claims
Preparing False Tax Returns

Offense Description

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.



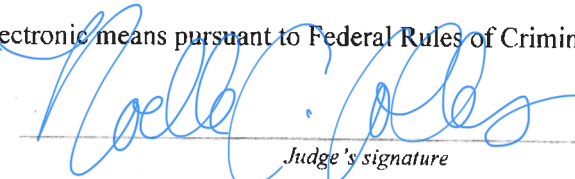
Applicant's signature

Nicholas D. Kenney, Special Agent, IRS

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date:

June 23, 2020

Judge's signature

City and state: St. Louis, MO

Noelle C. Collins, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH

Google, LLC email account:

SHELTONSTAXSERVICE@GMAIL.COM

THAT IS STORED AT PREMISES
CONTROLLED BY

Google, LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043

Case No. 4:20 MJ 3172 NCC

Filed Under Seal

SIGNED AND SUBMITTED TO THE
COURT FOR FILING BY RELIABLE
ELECTRONIC MEANS

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Nicholas D. Kenney, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Criminal Procedure 41 for information associated with a certain account that is stored at premises controlled by Google, LLC, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043 (hereinafter referred to as “the Provider”). The information to be searched is described in the following paragraphs and in Attachment A. The search warrant would require the Provider to disclose to the United States copies of the information (including the content of communications) further described in Attachment B. Upon receipt of the information described in Section I of Attachment B, United States-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the United States Department of the Treasury, Internal Revenue Service Criminal Investigation (IRS-CI) and have been so employed since June 2002. I am currently assigned to the St. Louis Field Office. I am a graduate of the Federal Law Enforcement Training Center and the IRS-CI National Academy. As a result of my training and experience as a Special Agent, I am familiar with federal laws. My primary duties have been the enforcement of federal laws pertaining to criminal tax violations and related financial crimes. I have worked on numerous criminal investigations including as the lead investigative agent. These investigations have included numerous income tax preparer fraud cases, like the one described below, that involved the electronic filing of false tax returns. During the course of these investigations, your affiant has planned, led, and participated in the execution of numerous search and arrest warrants, interviewed witnesses, conducted surveillance, and assisted during judicial proceedings, among other duties.

3. The information contained in this affidavit is based on my personal knowledge, information that I received from other agents and employees assisting in this investigation, and what I have learned from other sources specifically detailed herein. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 287 (filing false claims), and Title 26, United States Code, Section 7206(2) (preparing false tax returns) have been committed by Chantail Shelton and other individuals associated with Shelton's Tax Service, LLC. There is also probable cause to search the information described in

Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

LOCATION TO BE SEARCHED

5. The location to be searched is Sheltonstaxservice@gmail.com (herein referred to as “subject account”) located at 1600 Amphitheatre Parkway, Mountain View, California 64043, further described in Attachment A. The items to be reviewed and seized are described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the United States District Court for the Eastern District of Missouri is “a district court of the United States . . . that has jurisdiction over the offense being investigated” [18 U.S.C. § 2711(3)(A)(i)].

7. The presence of a law enforcement officer is not required for the service or execution of this warrant. 18 U.S.C. § 2703(g).

TRAINING AND EXPERIENCE OF INVESTIGATING AGENT

8. Based on your affiant’s knowledge, training and experience, your affiant knows that:

9. Income tax return preparer fraud schemes often involve patterns of false tax credits and tax deductions designed to maximize tax refunds for clients. Often tax return preparer schemes involving low-income clients include false claims for the federal Earned Income Tax Credit (“EITC”), which is a refundable tax credit available to taxpayers within a limited income range and who meet certain criteria. A refundable tax credit is one that can be

refunded to the taxpayer in excess of any tax due by the taxpayer. A taxpayer's income, filing status, and number of qualifying children are considered in an annual chart issued by the IRS specifying the EITC amount for which they qualify. For the 2019 tax year, for example, taxpayers with no qualifying children could receive an EITC amount of as much as \$529, taxpayers with one qualifying child could receive up to \$3,526, taxpayers with two qualifying children could receive up to \$5,828, and taxpayers with three qualifying children could receive as much as \$6,557. For the 2019 tax year, the EITC was available for individuals with an income range from \$1 to \$52,000, but taxpayers with qualifying children and with earned income amounts between roughly \$10,000 and \$19,000 were eligible for the highest EITC amounts.

10. Many tax return preparer schemes include the addition of false income or loss figures on individuals' tax returns in order to qualify those taxpayers to receive the EITC. Often these false figures appear on the Form 1040 Schedule C, "Profit or Loss From Business." This form is the form on which self-employed individuals report income and expense amounts related to their small businesses. In many schemes, preparers report false Schedule C business income for individuals lacking adequate legitimate income to qualify them for a significant EITC amount. Sometimes preparers also add fraudulent "household help" wage income to returns for the same purpose. Both the false Schedule C income and the false household help income are difficult to verify because the IRS does not routinely or necessarily receive substantiating records from third parties to document the income, in contrast to Forms W-2 documenting wage income from employers.

11. Conversely, in some schemes, preparers concoct false Schedule C business losses for clients who earn too much money legitimately, usually through wages reported on Forms W-2, to be eligible to receive the EITC. The reported Schedule C losses not only offset

the legitimate taxable income and eliminate any taxes due, they also place the clients' income within the range that qualifies them for the EITC.

12. Income tax return preparers sometimes charge and receive fees based on the number of schedules and the overall complexity of the returns. Often the tax return preparers perpetrating false refund schemes receive fees and other payments that are in excess of normal or average fees charged by legitimate tax return preparers. Word-of-mouth referrals among clients about the size of refunds available from a particular tax preparation business or individual tax return preparer often lead to additional customer volume for that business or preparer. Often income tax return preparers use third-party software and banks to process customer returns and refunds and tax preparation fees are often deducted directly from customer refunds before customers receive their refund payments.

BACKGROUND CONCERNING EMAIL

13. In my training and experience, I have learned that an email that is sent to an email subscriber of an email provider like Google, LLC is stored in the subscriber's "mail box" on the provider's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the provider's servers for a certain period of time.

14. In my training and experience, I have learned that Google, LLC provides a variety of on-line services, including electronic mail ("email") access, to the public. Google, LLC allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google, LLC. During the registration process, Google, LLC asks subscribers to provide basic personal

information. Therefore, the computers of Google, LLC are likely to contain stored electronic communications (including retrieved and unretrieved email for Google, LLC subscribers) and information concerning subscribers and their use of Google, LLC services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

15. A Google, LLC subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google, LLC. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

16. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

17. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This

information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

18. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of

occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

20. I have learned the following about Google:

- a. Google offers email services to the public. In particular, Google allows subscribers to maintain email accounts under the domain name gmail.com. A subscriber using the Google’s services can access his or her email account from any computer connected to the Internet.
- b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Device Information.* Google collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Android ID, Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated

Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

v. *Cookie Data.* Google uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user’s computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

vi. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google’s websites). Google also retains information regarding accounts registered from the same IP address.

vii. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber’s account.

viii. *Preserved and backup records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). Google may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

21. In addition, Google maintains records with respect to other Google Services, which it stores in connection with subscriber accounts, which typically include the following:

a. *Google Drive content.* Google provides users with a certain amount of free “cloud” storage, currently 15 gigabytes, through a service called “Google Drive” (users can purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content “in the cloud,” that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

b. *Google Docs.* Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called “Google Docs.” Users can use Google Docs to create online documents that can be stored on or saved to the user’s Google Drive.

c. *Google Photos.* Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or “Exif”) data, and can include GPS location information for where a photo or video was taken.

d. *Google Calendar.* Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered

computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

e. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in “chat” sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user’s email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user’s email and chat content.

f. *Location History data.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or “apps”) or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user’s location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device’s most recent location data in connection with a Google account.

g. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

h. *Google Profile.* Google allows individuals to create a Google profile with certain identifying information, including pictures.

i. *Google Plus.* Google hosts an Internet-based social network. Among other things, users can post photos and status updates and group different types of relationships (rather than simply “friends”) into Circles. In addition, Google has a service called PlusOne, in which

Google recommends links and posts that may be of interest to the account, based in part on accounts in the user's Circle having previously clicked "+1" next to the post. PlusOne information therefore provides information about the user of a given account, based on activity by other individuals the user has entered in the user's Circle.

j. *Chrome Browser and Search History.* Google stores information regarding user Internet browser activity when a Google user is logged into his or her account, which includes logging information about websites viewed by the user, Internet search queries in the Google Internet search engine available at <http://www.google.com> (and variations thereof, including <http://www.google.ru>), and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

k. *Advertising Data.* Google also stores advertising data, including information regarding unique advertising IDs associated with the customer, devices used to access the account, application IDs, advertising cookies, Unique Device Identifiers (UDIDs), payment information, ads clicked, and ads created.

l. *YouTube Data.* Google owns the video-streaming service YouTube and maintains records relating to YouTube accesses and data posted by the user.

PROBABLE CAUSE

Background

22. The Internal Revenue Service began reviewing the tax returns prepared by Shelton's Tax Service, LLC ("STS") in Ferguson, Missouri in April 2020 after a referral from another law enforcement agency in regard to one of the employees of the business. Investigation into STS revealed that it is owned by Chantail Shelton of St. Louis, Missouri. The business prepared tax returns for tax years 2018 and 2019 (prepared in calendar years 2019 and 2020).

Chantail Shelton was listed as the paid preparer on the majority of the returns in each year, but seven other individuals were listed as the paid preparer on at least one return prepared by STS in these years. Almost all of the tax returns were prepared and filed electronically with the Internal Revenue Service. Returns prepared and filed by STS claimed approximately \$4 million in refunds over the past two tax filing seasons.

23. The returns prepared by STS for the 2019 tax year (prepared in the first months of 2020) showed a very high refund rate of almost 99 percent. Of the 422 returns prepared by STS for the 2019 tax year, only 60 claimed refunds of less than \$1,000, and only 36 clients had refunds less than \$500. Returns filed by STS for the 2019 tax year reported that only five clients were owed a \$0 tax refund and no returns at all reported that clients owed additional tax to the IRS. Of the 291 electronically filed federal income tax returns prepared by STS for the 2018 tax year, only 16 clients had refunds of less than \$1,000 and only 7 had refunds of less than \$500. Four returns reported \$0 refunds and only two reported a tax due and owing to the IRS.

24. A large percentage of returns (just under 50%) filed by STS for the 2018 and 2019 tax years reported Schedule C losses. Almost all of these Schedule C losses coincided with taxpayers who were also reporting moderate to high wage amounts. For example, a nurse with the initials I.K. earning over \$120,000 in wages in 2018 and 2019 had Schedule C losses of over \$76,000 and \$65,000 in 2018 and 2019, respectively, for a purported home health care business. The result of these reported large Schedule C loss amounts was a drastic reduction in the taxpayer's tax liabilities and a resulting refund of over \$11,000 in each year. Other reported Schedule C losses were more subtle but no less suspicious. For example, one tax year 2019 return for a single taxpayer with initials V.C., who reported one qualifying child and reported approximately \$35,000 in wages and no federal withholdings, also reported an approximate

Schedule C loss of \$17,000 for a salon business. The taxpayer received the maximum available EIC amount and a refund of \$4,900. Without the Schedule C loss, the taxpayer would have received a much lower EIC amount and refund. This pattern of figures repeated itself on dozens of returns.

25. A large percentage of STS returns (approximately 40%) reported either Schedule C income or household help (“HSH”) income or both. This unsubstantiated income positioned many taxpayers for eligibility to receive the EITC. For example, the 2019 return of a single taxpayer with the initials S.G., with one qualifying child, reported no W-2 wages but \$11,503 in HSH income. The taxpayer received the maximum EITC available (\$3,526) and a refund of \$4,838. This pattern also repeated itself on dozens of returns.

26. Below is an overall summary of the federal income tax returns prepared by STS for the 2018 and 2019 tax years, as of May 28, 2020, followed by a breakdown of these figures by individual tax return preparer at the business.

2018 and 2019 Shelton’s Tax Service Returns

<u>Tax Year</u>	<u>Returns</u>	<u>Refund</u>	<u>EIC</u>	<u>Max EIC</u>	<u>Sch C Loss</u>	<u>Sch C Income</u>	<u>HSH</u>
2018	291	286	240	112	144	24	104
%		98.3%	82.5%	38.5%	49.5%	8.2%	35.7%
2019	422	417	338	143	209	43	144
%		98.8%	80.1%	33.9%	49.5%	10.2%	34.1%

2018 Shelton's Tax Service Returns by Preparer

<u>Preparer</u>	<u>Returns</u>	<u>Refund</u>	<u>EIC</u>	<u>Max</u> <u>EIC</u>	<u>Sch C</u> <u>Loss</u>	<u>Sch C</u> <u>Income</u>	<u>HSH</u>
Chantail Shelton	153	148	123	58	79	13	51
Charles Shelton	7	7	6	3	3	1	4
Chriselyn Mitchell	6	6	6	2	4	0	1
Courtney Williams	110	110	95	46	51	10	47
Denice Roach	11	11	9	3	6	0	1
Sharon Crawford	4	4	1	0	1	0	0
TOTAL	291	286	240	112	144	24	104

2019 Shelton's Tax Service Returns by Preparer

<u>Preparer</u>	<u>Returns</u>	<u>Refund</u>	<u>EIC</u>	<u>Max</u> <u>EIC</u>	<u>Sch C</u> <u>Loss</u>	<u>Sch C</u> <u>Income</u>	<u>HSH</u>
Chantail Shelton	301	298	251	114	142	36	113
Charles Shelton	13	13	13	6	5	3	6
Chriselyn Mitchell	2	2	2	2	1	0	1
Courtney Williams	41	41	32	9	18	2	15
Denice Roach	22	22	17	5	16	0	2
Jaquisha McCoy	2	2	1	0	2	0	0
Sharon Crawford	35	33	18	6	23	2	6
Tiffany Johnson	6	6	4	1	2	0	1
TOTAL	422	417	338	143	209	43	144

27. Below is a chart comparing the tax return characteristics of returns prepared by STS to the body of all tax returns prepared by a paid tax return preparer for the St. Louis metropolitan area (Missouri and Illinois counties), the state of Missouri, and the entire United States. These statistics were generated by a unit in the headquarters of Internal Revenue Service-Criminal Investigation charged with researching such information. Statistical information about the prevalence of household help income on tax returns was not available. An important note is

that the current filing season for tax returns for the 2019 tax year has been extended to July 15, 2020, so these statistics do not yet represent the entire 2020 filing season.

<u>Data Set</u>	<u>Characteristic</u>	<u>2018</u>		-	<u>2019</u>	
		<u>Count</u>	<u>%</u>		<u>Count</u>	<u>%</u>
STS Returns	Refund Return	291	98.3%	-	422	98.8%
St Louis Metro Area	Refund Return	461935	68.5%	-	335217	76.3%
State of Missouri	Refund Return	1004027	68.7%	-	741105	75.9%
All U.S. Returns	Refund Return	56780275	68.5%	-	40683617	78.3%
<u>Data Set</u>	<u>Characteristic</u>	<u>Count</u>	<u>%</u>	-	<u>Count</u>	<u>%</u>
STS Returns	EITC Claimed	291	82.5%	-	422	80.1%
St Louis Metro Area	EITC Claimed	87269	13.0%	-	66829	15.2%
State of Missouri	EITC Claimed	221953	15.2%	-	169310	17.3%
All U.S. Returns	EITC Claimed	13836331	16.7%	-	10529114	20.3%
<u>Data Set</u>	<u>Characteristic</u>	<u>Count</u>	<u>%</u>	-	<u>Count</u>	<u>%</u>
STS Returns	Schedule C Losses	291	49.5%	-	422	49.5%
St Louis Metro Area	Schedule C Losses	29122	4.3%	-	15928	3.6%
State of Missouri	Schedule C Losses	68896	4.7%	-	37545	3.8%
All U.S. Returns	Schedule C Losses	4246272	5.1%	-	2380766	4.6%
<u>Data Set</u>	<u>Characteristic</u>	<u>Count</u>	<u>%</u>	-	<u>Count</u>	<u>%</u>
STS Returns	Schedule C Profits	291	8.2%	-	422	10.2%
St Louis Metro Area	Schedule C Profits	87726	13.0%	-	44727	10.2%
State of Missouri	Schedule C Profits	205140	14.0%	-	106436	10.9%
All U.S. Returns	Schedule C Profits	13000774	15.7%	-	6338878	12.2%

28. It is your affiant's belief, based on your affiant's knowledge, training, and experience, that a sizable number of federal income tax returns prepared by Shelton's Tax Service for tax years 2018 and 2019 contained false and fraudulent information designed to minimize or eliminate tax liabilities for clients and/or maximize or greatly increase eligibility for refundable tax credits. Ultimately these items believed to be false significantly inflated clients' tax refunds. Particularly noteworthy and difficult to believe are the Schedule C losses reported on almost half of the returns prepared by STS over two years. Approximately 80 customers' returns prepared by STS reported Schedule C losses for both the 2018 and 2019 tax years, and

the strong majority of the loss amounts reported were in excess of \$10,000, and often well in excess of that amount, per return.

Physical and Internet Surveillance of Shelton's Tax Service

29. STS maintains a public Facebook page listing its office address as 299 S. Florissant Road in Ferguson, Missouri. The tax returns prepared by STS also listed this address as the "firm's address" in the paid preparer information section of the returns.

30. Your affiant observed a sign on the front door of STS from April 7, 2020 through May 6 with the following message: "Due to the coronavirus spread in Saint Louis, MO we are not in the office every day. If you have a concern or want to file please contact Chantail Shelton at (phone number). If we schedule an appointment with you please do not come if you are sick... We can do your taxes over the phone. If you have a check to be printed out of the office we will contact you as soon as your check is here and make prompt accommodations for you to pick up your check."

Undercover Operation

31. In early May 2020, the IRS initiated an undercover operation by assigning an undercover agent ("UCA") to pose as a prospective customer of Shelton's Tax Service. The UCA made telephonic and email contacts with Chantail Shelton over the next two weeks. These contacts resulted in Chantail Shelton's filing of a false 2019 federal income tax return for the UCA. The sequence of contacts was as follows.

32. On May 4, 2020, the UCA telephoned STS at the number posted on the front door of the physical location of STS and also on the STS Facebook page. The UCA explained to the unidentified female who answered the call that she was seeking tax preparation services. The unidentified female then instructed the UCA to send her by text message or by email the

following documents and information: identification, Forms W-2 or 1099, social security card, cellular telephone provider information, and email address. The unidentified female further explained, "So what I'll do is I'll work it up and see what it is first without doing anything to it, and straight putting it in, and then I'll call you and let you know and we'll just go from there."

33. Later in the evening on May 4, the UCA sent a text message to the same telephone number she had called earlier in the day and inquired about the email address to which she could send the documents and information needed to prepare the return. The UCA received the following response: Sheltonstaxservice@gmail.com. The UCA then, that same evening, emailed the following documents and information to that email address, Sheltonstaxservice@gmail.com: the Missouri driver's license for the UCA's covert identity; a social security card for the UCA's covert identity; a photograph of a Form W-2 bearing the UCA's covert name and identifying information, purporting to be issued by an employer in the St. Louis, Missouri area; the name of the UCA's cellular telephone provider; and the UCA's covert email address.

34. On the morning of May 6, the UCA contacted the STS telephone number again to follow up on the status of her tax return. Again an unidentified female answered the telephone. The unidentified female stated she was finishing up "everybody's" returns and asked the UCA to give her an hour or so to complete it. The female then asked the UCA whether she would be claiming any dependents and the UCA responded, "No." The female asked whether the UCA had a "side gig or anything that you do?" The UCA responded that she did not really have any side jobs, though she occasionally did somebody's hair, but nothing regular or consistent. The female said, "No, that'll help." The UCA explained that she didn't know how much she earned from this hair styling work, she did braids every now and then, she did not purchase supplies,

and she wasn't keeping track of it. The female then commented that she was trying to be very quiet so she did not wake up her kids. The UCA and the female then decided the UCA should call back for an update on the return later in the afternoon.

35. On the afternoon of May 6, the UCA attempted to call STS but no one answered. The UCA left a voicemail asking for a return call. Approximately 40 minutes later, a woman identifying herself as Chantail Shelton called the UCA. Shelton told the UCA, "When I put everything in, it came up that you were getting back \$30 from federal and \$20 from state." The UCA said, "Thirty dollars?" Shelton continued, "But if I put in something like you did hair and did some extensions, then, uh, after fees it came up to \$1,504 from federal and then \$990 from state." Shelton asked whether the UCA wanted direct deposit for the refunds and the UCA provided Shelton with a routing number and bank account number. Shelton told the UCA she was done with preparing the return. The UCA inquired about the tax preparation fee and Shelton explained that the fee would come out of the UCA's refund and the refund figures Shelton had just given to the UCA represented the amounts the UCA would receive after fees had been deducted.

36. On May 6, the IRS received an electronically filed 2019 federal income tax return bearing the UCA's covert identifying information and listing the paid preparer as Chantail Shelton and the preparer firm as Shelton's Tax Service. The return reported the wages and federal tax withholdings from the Form W-2 the UCA had provided to Shelton. The return also reported a false Schedule C loss of \$20,032. The Schedule C, "Profit or Loss From Business," reported \$0 in gross receipts for the UCA's purported hair styling business and \$9,851 in car and truck expenses, \$2,065 in contract labor expenses, \$4,036 in supply expenses, \$2,015 in travel expenses, and \$2,065 in business cell phone expenses. The UCA had provided none of these

expense figures to Shelton during their telephone, email, or text message contacts. This tax return claimed a refund of \$2,339. If the return had been prepared accurately, with only the wages on the Form W-2 and not the Schedule C loss, the return should have claimed a federal tax refund of only \$30.

37. On May 11, the UCA sent an email to Sheltonstaxservice@gmail.com to request a copy of the UCA's income tax return. The UCA did not receive a reply. On May 15, the UCA called STS and spoke to a female believed to be Chantail Shelton. The UCA again requested that Shelton email a copy of the tax return to her. Shelton agreed to email the return.

38. Later on May 15, the UCA received an email from the address Sheltonstaxservice@gmail.com. The email contained a file attachment of the UCA's 2019 federal income tax return that matches the tax return for the UCA filed with the IRS. The file contained a copy of the UCA's 2019 Missouri state income tax return, the key figures of which matched the federal return. The file contained a fee disclosure form showing the UCA would have been charged a total of \$669.99 in tax preparation fees and another \$164.90 in various other processing fees. At the bottom of the email from Sheltonstaxservice@gmail.com was the following information:

Chantail Shelton-Owner
Shelton's Tax Service
299 S. Florissant Road
Ferguson, MO 63135
sheltonstaxservice@gmail.com
(Phone Number)

39. A preservation letter was sent to Google, LLC on June 9, 2020 to request that all email content and other account data for the account sheltonstaxservice@gmail.com be preserved for at least 90 days.

CONCLUSION

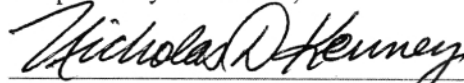
40. Based on the foregoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on the Provider. Because the warrant will be served on the Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

41. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under penalty of perjury that the foregoing is true and correct.

Respectfully submitted,



Nicholas D. Kenney, Special Agent
Department of Treasury
IRS - Criminal Investigation

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal

Rules of Criminal Procedure 4.1 and 41 on this 23rd **day of June, 2020.**


HONORABLE NOELLE C. COLLINS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **Sheltonstaxservice@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered at:

Google, LLC

1600 Amphitheatre Parkway

Mountain View, California 94043

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on June 9, 2020, the Provider is required to disclose the following information, for the time period January 1, 2019 through May 31, 2020, to the government for each account or identifier listed in Attachment A:

- a. The content of all communications associated with the account, including through Gmail, Google Hangouts (including videos), and otherwise, all emails sent to and from the account, emails stored in draft form in the account, the date and time at which each email was sent or received, the size and length of each email, and including all message content, attachments, and header information;
- b. All address book, contact list, or similar information associated with the account;
- c. Full Google search history and Chrome browser history associated with the account;
- d. All Google Drive content;
- e. All bookmarks maintained by the account;
- f. All services used by the account;
- g. All subscriber and payment information, including full name, e-mail address (including any secondary or recovery email addresses), physical address (including city, state, and

zip code), date of birth, gender, hometown, occupation, telephone number, websites, screen names, user identification numbers, security questions and answers, registration IP address, payment history, and other personal identifiers;

h. All past and current usernames, account passwords, and names associated with the account;

i. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;

j. All YouTube data associated with the account;

k. All transactional records associated with the account, including any IP logs or other records of session times and durations;

l. Any information identifying the device or devices used to access the account, including a device serial number, a GUID or Global Unique Identifier, Android ID, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”), and any other information regarding the types of devices used to access the account;

m. All activity logs for the account;

n. All photos and videos uploaded to the account, including in Google Drive and Google Photos;

o. All information associated with Google Plus, including the names of all Circles and the accounts grouped into them;

- p. All photos and videos uploaded by any user that have that user tagged in them;
- q. All location and maps information;
- r. All Google Voice information;
- s. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- t. All privacy settings and other account settings, including email addresses or other accounts that the account has blocked;
- u. Advertising and Device Data: All advertising data relating to the account, including, but not limited to, advertising cookies, information regarding unique advertising IDs associated with the user, any devices used to access the account, Android IDs, application IDs, UDIDs, payment information (including, but not limited to, full credit card numbers and expiration dates and PayPal accounts), ads clicked, and ads created;
- v. Linked Accounts: All accounts linked to the Target Account (including where linked by machine cookie or other cookie, creation or login IP address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise);
- w. For accounts linked by cookie, the date(s) on which they shared a cookie;
- x. For accounts linked by SMS number, information regarding whether the numbers were verified; and
- y. Customer Correspondence: All records pertaining to communications between the Service Provider and any person regarding the user or the user's account with the Service Provider, including contacts with support services, records of actions taken, and investigative or user complaints concerning the subscriber; and

z. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 287 (conspiracy to file false claims and filing false claims), and Title 26, United States Code, Section 7206(2) (assisting in the preparation of false tax returns.), those violations involving Chantail Shelton and others known and unknown and occurring on or after January 1, 2019 through May 31, 2020, including, for the account listed on Attachment A, information pertaining to the following matters:

- (a) Evidence regarding the transmission of personally identifiable information and records for the purpose of filing personal and business income tax returns; tax returns and related forms and schedules; questions and information from taxpayers or from tax return preparers regarding the filing of tax returns; communications among tax return preparers regarding the preparation of tax returns; communications among tax return preparers and clients regarding fees and payments related to the preparation of tax returns;
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters related to the preparation and filing of false tax returns, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any United States personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, analysts, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agents may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the United States and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, LLC, and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google, LLC. The attached records consist of _____ (pages/CDs/megabytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, LLC, and they were made by Google, LLC as a regular practice; and

b. such records were generated by Google, LLC electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google, LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature